UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,024	10/29/2003	Jin Mu Wu	430151.401	7163

500 7590 03/07/2007
SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVE
SUITE 5400
SEATTLE, WA 98104

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/698,024	**Applicant(s)** WU, JIN MU
	Examiner Carl Colin	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *see att*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-10 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 8/2/2005 being considered by the examiner.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Malaysia on 10/29/2002. It is noted, however, that applicant has not filed a certified copy of the PI 20024037 application as required by 35 U.S.C. 119(b)..

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,772,343 to **Shimizu et al** in view of US Patent 5,710,813 to **Terui et al.**

As per claim 1, Shimizu et al substantially discloses a method of encrypting binary data using block encryption and a private key, the method comprising: a key transformation section generating a series of coding transforms using a secret key in a repeatable manner such as to produce an mth row (see column 6, lines 30-39) that meets the recitation of *generating a series of coding transforms using said private key, said series of coding transforms being generated in a repeatable manner;* and discloses *encrypting blocks of said binary data by selectively applying said coding transforms* (see column 6, lines 30-39 and column 7, lines 17-23). **Shimizu et al** does not explicitly disclose modifying elements within a block of the binary data to be encrypted. **Terui et al** in an analogous art teaches a method of encrypting binary data wherein the plaintext data is being modified by a transposition function and an inversion function (see figure 7) and discloses generating coding transform *adapted to modify elements within a block of said binary data to be encrypted* (see column 6, lines 7-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Shimizu et al** to modify elements of the data to be encrypted as suggested by **Terui et al**. One skilled in the art would have been lead to make such a modification because modifying elements within a block of the binary data before or during encryption gives an unexpectedly raised degree of secrecy to the encrypted data.

As per claim 2, the references as combined above disclose the limitation of *wherein a different coding transform of said series is used to encrypt each said block* (see **Shimizu et al**, column 11, lines 40-50).

As per claim 3, the references as combined above disclose the limitation of *wherein sequentially generated coding transforms of said series are used to encrypt sequential blocks containing said binary data* (see **Shimizu et al**, column 7, lines 17-23).

As per claim 4, the references as combined above disclose the limitation of *wherein each coding transform of said series is adapted to transpose elements within the block of binary data to be encrypted* (see **Terui et al**, column 6, lines 24-32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Shimizu et al** to transpose elements of the data to be encrypted as suggested by **Terui et al**. One skilled in the art would have been lead to make such a modification because transposing elements within a block of the binary data before or during encryption gives an unexpectedly raised degree of secrecy to the encrypted data.

As per claim 5, the references as combined above disclose the limitation of *wherein each coding transform of said series is adapted to selectively invert ones of said elements within the block of binary data to be encrypted* (see **Terui et al**, column 6, lines 24-32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Shimizu et al** to inverting elements of the data to be encrypted as suggested by **Terui**

et al. One skilled in the art would have been lead to make such a modification because inverting elements within a block of the binary data before or during encryption gives an unexpectedly raised degree of secrecy to the encrypted data.

As per claim 6, the references as combined above disclose the limitation of *wherein each coding transform of said series is adapted to transpose elements within a block of binary data to be encrypted and to selectively invert ones of those elements* (see **Terui et al**, column 6, lines 24-32). Claim 6 is therefore rejected on the same rationale as the rejection of claims 4 and 5 above.

As per claim 7, the references as combined above disclose the limitation of *wherein each coding transform of said series is generated as one sub-transform for achieving the transposition function and another sub-transform for achieving the inversion function, and wherein said sub-transforms are applied in any order in the encrypting step* (see **Terui et al**, column 6, lines 24-32). Claim 7 is therefore rejected on the same rationale as the rejection of claims 4 and 5 above.

As per claim 8, the references as combined above disclose the limitation of *wherein said series of coding transforms is generated in a pseudo-random manner* (see **Shimizu et al**, column 6, lines 30-39 and column 7, lines 4-10).

As per claim 9, the references as combined above disclose encryption apparatus for performing the method of claim 1 and further discloses a computer and encryption processor comprising memory (input buffer) for receiving plain blocks of binary data to be encrypted (see **Shimizu et al**, figure 1 and column 15, line 62-63); an input register for receiving said private key (see **Shimizu et al**, fig.1, key transformation unit 12); an arithmetic unit for generating a series of control outputs, corresponding to said series of coding transforms, using said private key (see **Shimizu et al**, column 6, lines 26-39); logic circuitry, responsive to said series of control outputs, for converting input plain blocks of binary data to encrypted blocks of binary data in accordance with said series of coding transforms and an output buffer (memory) for outputting said encrypted blocks of binary data (see **Shimizu et al**, figure 1 and column 10, lines 42-49).

As per claim 10, the references as combined above disclose a computer program product for encrypting binary data using block encryption and a private key, the product comprising program code constituting a set of instructions for performing the method of claim 1 and further discloses implementing the invention in a hardware and software using program product executed by processor or computer (see **Shimizu et al**, column 15, line 59 through column 6, line 2).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses encrypting binary data using block encryption and private key and some of the claimed features such as modifying elements within a block of binary data to be encrypted. See PTO form 892.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
March 4, 2007